Remarks/Arguments

Claims 1-14 are pending in the application. Claims 1-14 are rejected. Claims 1 and 5 have been cancelled and claims 2, 4, 6, 7 and 9-14 have been amended to further define the claimed subject matter. No new matter has been added.

Claim Objections Under 37 CFR § 1.75(c)

Claim 14 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. Claim 14 has been amended to address this objection.

Claim Rejections Under 35 USC § 112

Claim 5 is rejected under 35 USC 112, first paragraph, as failing to comply with the enablement requirement. Claim 5 has been cancelled.

Claims 1, 6, and 10 are rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 has been cancelled and claims 6 and 10 have been amended to address this rejection.

Claim Rejections Under 35 USC § 102

Claims 1, 4-5, 7 and 9-12 are rejected under 35 USC 102(e) as being anticipated by Patarin et al. (6,658,569). Claims 1 and 5 have been cancelled and claims 4, 7 and 9-12 have been amended to address this rejection so as to not further delay the prosecution of this application. Applicant reserves the opportunity to prosecute original claims 1, 4-5, 7 and 9-12 in a subsequent application to include appropriate affidavits and evidence of prior invention over the Patarin reference.

Claim Rejections Under 35 USC § 103

Claims 2, 4-5, and 13 are rejected under 35 USC 103(a) as being unpatentable over Patarin as applied to claims 1 and 12 above, and further in view of Jahnich et al. (6,725,374). Regarding claims 2 and 13, the Office action provides that the Patarin reference does not teach the use of dummy operations in cryptography.

The Office action asserts that the use of dummy programs as taught in Jahnich, whose execution does not influence an encryption result, meet the limitation of dummy operations, and that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Patarin to use dummy operations as taught by Jahnich. Applicant respectfully traverses this ground for rejection for the reasons given below.

Applicant respectfully submits that, in Jahnich, the execution of the encryption program is in "serial order of execution of at least two subprograms [is] randomly permuted in the execution of the encryption program under the consideration of at least one random number". (Abstract) "[E]ach program level could be extended by such a number of "dummy subprograms" that the number of subprograms in each program level is the same." (Col. 6, lines 53-56)

Applicant submits that it would not be obvious to one skilled in the art to apply the "dummy programs" that are used for the injection of "dummy subprograms" within the serial order of execution of at least two of a plurality of parallelisationable subprograms of an encryption program as taught in Jahnich, for parallel and simultaneous execution of cryptographic sub-operations and dummy operations as provided in Applicant's claims. The serial execution of dummy programs with subprograms is not suggestive and does not teach the advantages of a parallel and simultaneous execution of dummy operations and sub-operations of an encryption program.

In addition, Applicant respectfully submits that there would be no obvious recognition that the current fluctuations observed in a DPA analysis in the serial execution of dummy programs with subprograms would be advantageous, useful, or successful in the obscuring of the current signature of a parallel and simultaneous execution of dummy operations and sub-operations. The current signature of dummy programs injected in a serial execution of subprograms are uniquely distinct and would obscure in a very different mode and mechanism as compared with the current signature of parallel and simultaneous execution of dummy operations and sub-operations.

Amended independent claims 2, 4, 7, 10 and 13 include the limitation in various forms wherein there is a parallel and simultaneous execution of dummy operations and sub-operations. For the reasons stated above, Applicant submits that this limitation is not provided by the combination of Patarin in view of Jahnich. Applicant respectfully requests reconsideration and allowance of claims 2, 4, 7, 10 and 13.

Claim 3 depend from claim 2, claim 6 depends from claim 4, claim 8 and 9 depend from claim 7, claims 11 and 12 depend from claim 10, and claim 14 depends from claim 13, and are further limitations of respective independent claims, therefore, claims 3, 6, 8, 9, 11, 12 and 14 are not obvious in view of Patarin and Jahnich for the reasons given above. Applicant respectfully requests reconsideration and allowance of claims 3, 6, 8, 9, 11, 12 and 14.

Claims 3-6 and 14 are rejected under 35 USC 103(a) as being unpatentable over Patarin in view of Jahnich as applied to claims 2, 7 and 13 above, and further in view of Tan (6,490,353). Claims 8-9 are rejected under 35 USC 103(a) as being unpatentable over Patarin as applied to claim 7 above, and further in view of Tan. Tan does not teach the use of dummy operations as provided in applications claims and therefore the addition of Tan does not render the claims obvious, as discussed above.

Documents Cited but Not Relied upon for this Office Action

Applicant need not respond to the assertion of pertinence stated for the references cited but not relied upon by the Office Action since these references are not made part of the rejections in this Office Action. Applicant is expressly not admitting to this assertion and reserves the right to address the assertion should it form part of future rejections.

In view of the foregoing reasons for distinguishing over the cited reference, Applicant has not raised other possible grounds for traversing the rejections, and therefore nothing herein should be deemed as acquiescence in any rejection or waiver of arguments not expressed herein

CONCLUSION

Applicant submits that in view of the foregoing remarks and/or amendments, the application is in condition for allowance, and favorable action is respectfully requested. The Commissioner is hereby authorized to charge any fees, including extension fees, which may be required, or credit any overpayments, to Deposit Account No. 50-1001.

Respectfully submitted,

Date: December 16, 2004

Paul J. Fordenbacher
Registration No. 42,546
P. O. Box 2200
Hillsboro, OR 97123
Telephone: (503) 844-9009
Facsimile: (503) 296-2172
email: mail@ganzlaw.com

Correspondence to:

Philips Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131 USA
Telephone: (408) 474-9073
Facsimile: (408) 474-9082
USPTO Customer Number: 24738